IPAS-BUS 09.03.2009

HIT: 2 OF 2, Selected: 0 OF 0

© Thomson Scientific Ltd. DWPI

Accession Number
1998-063493

Title Derwent
Key sequence establishment method for secure communications through transceiver channel - using impedances of channel viewed from each transceiver to other with keys set equivalent to bounded distance decoding, incorporating tone group transmissions to identify phase differences

Abstract Derwent
Unstructured:
The method involves operating a first transceiver to transmit multiple tones, each tone having a predetermined frequency and initial phase. These are received by the second receiver and transmitted back, the second receiver also transmitting a second set of tones similar to the first. The first transceiver receives these and transmits them back and finds the differences between the phases of pairs of the first tones, quantising each difference into a phase decision value. It decodes the quantised differences into a key sequence according to a predetermined block code. The second transceiver finds the difference between tone phase pairs, quantises them into phase decision values and decodes the quantised differences into the key sequence. For communicating financial information with reduced susceptibility to eavesdropping. Uses channel characteristics to establish and exchange cryptographic keys with almost perfect secrecy. Impedance characteristics are generally not identical in non-reciprocal channel. No need for each party to generate pseudo-random quantity. By using channel decoder, probability of two users establishing same secret key is close to one, while probability of eavesdropper establishing same key is essentially zero. Number of possible keys is large enough that finding correct one by exhaustive search is impractical.

Assignee Derwent + PACO
ERICSSON INC TELF-S

Assignee Original
Ericsson Inc.
Ericsson Inc.
Ericsson Inc.

Inventor Derwent

CHENNAKESHU S	HASSAN A
HASSAN A A	HERSHEY E
HERSHEY J	HERSHEY J E

Patent Family Information

WO1997049213-A1	1997-12-24	AU9731511-A	1998-01-07
US5745578-A	1998-04-28	TW341015-A	1998-09-21
EP906679-A1	1999-04-07	CN1222275-A	1999-07-07
US6031913-A	2000-02-29	AU723304-B	2000-08-24
JP2000512825-W	2000-09-26	KR2000016713-A	2000-03-25
CN1104119-C	2003-03-26	EP906679-B1	2006-08-09
DE69736471-E	2006-09-21	IN9701526-I1	2007-02-23

JP3963280-B2 2007-08-22 DE69736471-T2 2007-09-20

First Publication Date 1997-12-24

Priority Information

US000665339 1996-06-17 US000015774 1998-01-29

Derwent Class

P85 W01

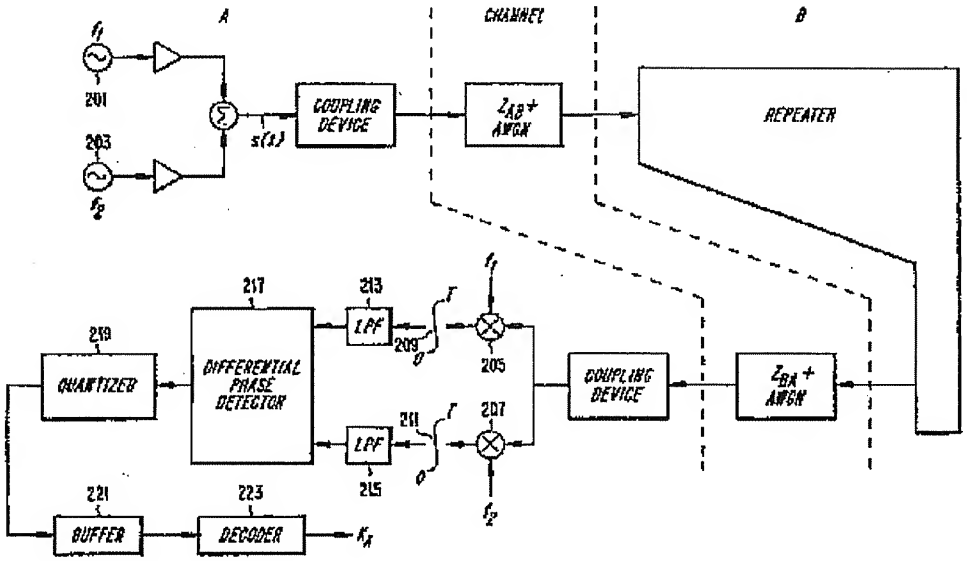
Manual Code

W01-A05A

International Patent Classification (IPC)

IPC Symbol	IPC Rev.	Class Level	IPC Scope
G09C-1/00	2006-01-01	I	C
H04L-9/08	2006-01-01	I	C
H04L-9/08	2006-01-01	I	C
H04L-9/08	2006-01-01	I	C
H04L-9/12	2006-01-01	I	C
G09C-1/00	2006-01-01	I	A
H04L-9/08	2006-01-01	I	A
H04L-9/08	2006-01-01	I	A
H04L-9/08	2006-01-01	I	A
H04L-9/12	2006-01-01	I	A
H04L-9/00	-		
H04L-9/06	-		
H04L-9/08	-		

Drawing



[19]中华人民共和国国家知识产权局

[51]Int.Cl[6]
H04L 9/08

[12]发明专利申请公开说明书

[21]申请号 97195569.7

[43]公开日 1999年7月7日

[11]公开号 CN 1222275A

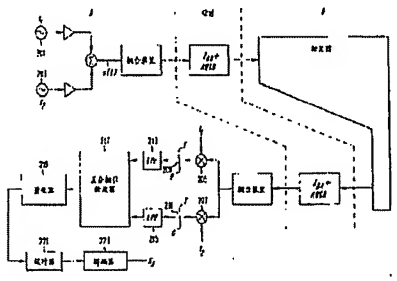
[22]申请日 97.6.6 [21]申请号 97195569.7
[30]优先权
[32]96.6.17 [33]US [31]08/665,339
[86]国际申请 PCT/US97/09348 97.6.6
[87]国际公布 WO97/49213 英 97.12.24
[85]进入国家阶段日期 98.12.16
[71]申请人 艾利森公司
地址 美国北卡罗莱纳州
[72]发明人 A·A·哈桑 J·E·赫尔希
S·岑纳克苏
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 栾本生 李亚非

权利要求书6页 说明书15页 附图页数4页

[54]发明名称 基于信道特征的安全通信的装置与方法

[57]摘要

利用通信信道的特征来建立密钥序列供在加密传递的信息中使用。在一个实施 例中,这些特征为从一台收发机向另一台观察的及反过来观察的信道阻抗。这 些密钥可用等价于限定距离解码过程的计算建立,且用于建立密钥的解码器可 用来处理以后的数据传输。与古典的及公开密钥密码系统相比,提供了用于建 立依赖于物理过程的共享密钥序列的替代机制,其中各方不需要生成伪随机量 ,因为必要的随机性是由通信信道本身的性质提供的。通过使用信道解码器, 两个用户建立相同的秘密密钥的概率基本上为1,而窃听者建立相同密钥的概 率基本上为零。同时,可能的密钥的数目大到足以使用穷举搜索找到正确的密 钥是不现实的。



ISSN1008-4274

权　利　要　求　书

1. 一种为通过第一收发机与第二收发机之间的通信信道的安全通信建立密钥序列的方法，包括下述步骤：

在第一收发机中，发送第一多个音调，各音调具有各自的预定频率及预定的初相；

在第二收发机中，接收第一收发机所发送的第一多个音调并基本上不加改变地将接收的第一多个音调发送回第一收发机；

在第二收发机中，发送第二多个音调，各音调具有各自的预定频率及预定的初相；

在第一收发机中，接收第二多个音调并基本上不加改变地将接收的第二多个音调发送回第二收发机；

在第一收发机中，确定所接收的第一多个音调的对的相位之间的差，将各差量化成多个相位判定值中各自的一个；并按照预定的块码将多个量化的差解码成密钥序列；以及

在第二收发机中，确定所接收的第二多个音调的对的相位之间的差，将各差量化成多个相位判定值中各自的一个；并按照预定的块码将多个量化的差解码成密钥序列；

2. 根据权利要求 1 的方法，还包括，在各第一与第二收发机中，确定其各自接收的多个音调中各个的幅值的步骤，其中这些幅值在解码步骤中用作软信息。

3. 根据权利要求 1 的方法，还包括，在第一与第二收发机中至少一个中，按照该密钥序列加密要传输的信息的步骤；以及在第一与第二收发机的至少另一个中，按照该密钥序列解密加密的传输的信息的步骤。

4. 根据权利要求 3 的方法，其中的加密步骤包括在流密码系统中组合密钥序列与要传输的信息的步骤。

5. 根据权利要求 3 的方法，其中的加密步骤包括在面向块的密码系统中组合密钥序列与要传输的信息的步骤。

6. 一种用于为通过第一收发机与第二收发机之间的通信信道的安全通信建立密钥序列的装置，包括：

在第一收发机中，用于发送第一多个音调的装置，各音调具有各自的预定频率及预定的初相；

在第二收发机中，用于接收第一收发机发送的第一多个音调并基本上不加改变地将所接收的第一多个音调发送回第一收发机的装置；

在第二收发机中，用于发送第二多个音调的装置，各音调具有各自的预定频率及预定的初相；

在第一收发机中，用于接收第二多个音调及基本上不加改变地将所接收的第二多个音调发送回第二收发机的装置；

在第一收发机中，用于确定所接收的第一多个正弦波信号的对的相位之间的差的装置；用于将各差量化成多个相位判定值中各自的一个的装置；及用于按照预定的块码将多个量化的差解码成密钥序列的装置；以及

在第二收发机中，用于确定所接收的第二多个正弦波信号的对的相位之间的差的装置；用于将各差量化成多个相位判定值中各自的一个的装置；及用于按照预定的块码将多个量化的差解码成密钥序列的装置；

7. 根据权利要求 6 的装置，还包括，在各第一与第二收发机中，用于确定其各自的所接收的多个音调中各个的幅值的装置，其中的解码装置将这些幅值用作软信息。

8. 根据权利要求 6 的装置，还包括，在第一与第二收发机中至少一个中，用于按照密钥序列加密要传输的信息的装置；及在第一与第二收发机的至少另一个中，用于按照密钥序列解密加密的传输的信息的装置。

9. 根据权利要求 8 的装置，其中的加密装置包括用于在流密码系统中组合密钥序列与要传输的信息的装置。

10. 根据权利要求 8 的装置，其中的加密装置包括用于在面向块的密码系统中组合密钥序列与要传输的信息的装置。

11. 一种为通过第一收发机与第二收发机之间的通信信道的安全通信建立密钥序列的方法，包括下述步骤：

在第一收发机中，传输包含多位的第一预定数字字；

在第二收发机中，接收第一预定数字字并基本上不加改变地将接收的第一预定数字字传输回第一收发机；

在第二收发机中，传输包含多位的第二预定数字字；

在第一收发机中，接收第二预定数字字并基本上不加改变地将接收的第二预定数字字传输回第二收发机；

在第一收发机中，硬判决解码从第二收发机接收的第一预定数字字中多位中的各位；并按照预定的块码将硬判决解码的多位映射到密钥序列中；以及

在第二收发机中，硬判决解码从第一收发机接收的第二预定数字字中的多位中的各位；及按照预定的块码将硬判决解码的多位映射到密钥序列中。

12. 根据权利要求 11 的方法，还包括，在各第一与第二收发机中，确定其各自接收的预定数字字的多位中各位的幅值的步骤，其中这些幅值在映射步骤中用作软信息。

13. 根据权利要求 11 的方法，还包括，在第一与第二收发机中至少一个中，按照密钥序列加密要传输的信息的步骤；及在第一与第二收发机中的至少另一个中，按照密钥序列解密加密的传输的信息的步骤。

14. 根据权利要求 13 的方法，其中的加密步骤包括在流密码系统中组合密钥序列与要传输的信息的步骤。

15. 根据权利要求 13 的方法，其中的加密步骤包括在面向块的密码系统中组合密钥序列与要传输的信息的步骤。

16. 一种用于为通过第一收发机与第二收发机之间的通信信道的安全通信建立密钥序列的装置，包括：

在第一收发机中，用于传输包含多位的第一预定数字字的装置；

在第二收发机中，用于接收第一收发机所传输的第一预定数字字的装置，及用于基本上不加改变地将所接收的第一预定数字字传输回第一收发机的装置；

在第二收发机中，用于传输包含多位的第二预定数字字的装置；

在第一收发机中，用于接收第二收发机传输的第二预定数字字的装置，及用于基本上不加改变地将接收的第二预定数字字传输回第二收发机的装置；

在第一收发机中，用于硬判决解码从第二收发机接收的第一预定数字字中的多位中的各位的装置；及用于按照预定的块码将硬判决解码的多位映射到密钥序列中的装置；以及

在第二收发机中，用于硬判决解码从第一收发机接收的第二预定数字字中的多位中的各位的装置；及用于按照预定的块码，将硬判决解码的多位映射到密钥序列中的装置；

17.根据权利要求16的装置，还包括，在各第一与第二收发机中，用于确定其各自接收的预定数字字的多位中的各位的幅值的装置，其中这些幅值由映射装置用作软信息。

18.根据权利要求16的装置，还包括，在第一与第二收发机中至少一个中，用于按照密钥序列加密要传输的信息的装置；及在第一与第二收发机中的至少另一个中，用于按照密钥序列解密加密的传输的信息的装置。

19.根据权利要求18的装置，其中的加密装置在流密码系统中组合密钥序列与要传输的信息。

20.根据权利要求18的装置，其中的加密装置在面向块的密码系统中组合密钥序列与要传输的信息。

21.一种为通过第一收发机与第二收发机之间的通信信道的安全通信建立密钥序列的方法，包括下述步骤：

在第一收发机中，传输包含多位的第一预定数字字；

在第二收发机中，接收第一收发机传输的第一预定数字字，并基本上不加改变地将接收的第一预定数字字传输回第一收发机；

在第二收发机中，传输包含多位的第二预定数字字；

在第一收发机中，接收第二收发机传输的第二预定数字字，并基本上不加改变地将接收的第二预定数字字传输回第二收发机；

在第一收发机中，确定从第二收发机接收的第一预定数字字的多位中各位的相位；确定各确定的相位与各自的预定相位之间的差；将各差量化成多个相位判定值中各自的一个；及按照预定的块码将多个量化的差解码成密钥序列；以及

在第二收发机中，确定从第一收发机接收的第二预定数字字的多位中各位的相位；确定各确定的相位与各自的预定相位之间的差；将各差量化成多个相位判定值中各自的一个；及按照预定的块码将多个量化的差解码成密钥序列。

22.根据权利要求21的方法，还包括，在各第一与第二收发机中，确定其各自接收的预定数字字的多位中的各位的幅值的步骤，其中这

些幅值在解码步骤中用作软信息。

23. 根据权利要求 21 的方法，还包括，在第一与第二收发机中至少一个中，按照密钥序列加密要传输的信息的步骤；及在第一与第二收发机中至少另一个中，按照密钥序列解密加密的传输的信息的步骤。

24. 根据权利要求 23 的方法，其中的加密步骤包括在流密码系统中组合密钥序列与要传输的信息的步骤。

25. 根据权利要求 23 的方法，其中的加密步骤包括在面向块的密码系统中组合密钥序列与要传输的信息的步骤。

26. 一种用于为通过第一收发机与第二收发机之间的通信信道的安全通信建立密钥序列的装置，包括：

在第一收发机中，用于传输包含多位的第一预定数字字的装置；

在第二收发机中，用于接收第一收发机传输的第一预定数字字的装置，及用于基本上不加改变地将接收的第一预定数字字传输给第一收发机的装置；

在第一收发机中，用于确定从第二收发机接收的第一预定数字字的多位中各位的相位的装置；用于确定各确定的相位与各自的预定相位之间的差的装置；用于将各差量化成多个相位判定值中各自的一个的装置；及用于接照预定的块码将多个量化的差解码成密钥序列的装置；以及

在第二收发机中，用于确定从第一收发机接收的第二预定数字字的多位中的各位的相位的装置；用于确定各确定的相位与各自的预定相位之间的差的装置；用于将各差量化成多个相位判定值中各自的一个的装置；及用于按照预定的块码将多个量化的差解码成密钥序列的装置。

27. 根据权利要求 26 的装置，还包括，在各第一与第二收发机中，用于确定其各自接收的预定数字字的多位中各位的幅值的装置，其中这些幅值由解码装置用作软信息。

28. 根据权利要求 26 的装置，还包括，在第一与第二收发机中至少一个中，用于按照密钥序列加密要传输的信息的装置；及在第一与第二收发机中的至少另一个中，用于按照密钥序列解密加密的传输的信息的装置。

29. 根据权利要求 28 的装置，其中的加密装置在流密码系统中组合密钥序列与要传输的信息。

30. 根据权利要求 28 的装置，其中的加密装置在面向块的密码系统中组合密钥序列与要传输的信息。

说　明　书

基于信道特征的安全通信的装置与方法

本申请人的发明涉及通过诸如电话线等具有非互易或互易特征的通信链路的安全传递信息的装置与方法，这便是说降低窃听的敏感性。

对安全通信系统的广泛需求是显而易见的。只作为一个例子，金融交易是例行通过电话线进行的。在这一和许多其它实例中，尽管潜在的窃听者能接近强信息信号，用几乎完美的保密性进行信息通信是关键的。

提供安全性的一种方法是按照用户事先同意使用的某一系统来加密传递的信息。文献中已描述过多种加密方法，诸如数据加密标准（DES）及公开密钥加密术（PKC）。如在 W.Diffie 等人的“保密与鉴别：密码学导论”IEEE 学报卷 67，397－427 页（1979 年 3 月）中所述，古典密码系统通常是能以各种方式将明文（未加密的信息）转换成密文或反过来的一组指令、一个硬件或计算机程序，其中之一为用户知道而对其它人保密的特定密钥所选择的。DES 便是一种古典的密码系统。

流行的 PKC 系统利用寻找大素数是计算上容易的而分解两个大素数之积是计算上困难的这一事实。PKC 系统超过诸如 DES 等其它密码系统的优点在于 PKC 系统使用不同于加密密钥的解密密钥。从而，PKC 用户的加密密钥可公开供他人使用，而避免了安全地分配密钥的困难。见诸如 R.I.Rivest 等人的“获取数字签名与公开密钥密码系统的方法”，ACM 通讯卷 21，120－126 页（1978 年 2 月）；及 W.Diffie 的“公开密钥密码系统的前十年”，IEEE 学报卷 76，560－577 页（1988 年 5 月）。

对于古典的或 PKC 系统，报文的安全性在极大程度上取决于密钥的长度，如在 C.E.Shannon 的“保密系统的通信理论”Bell Sys.Tech.J. 卷 28，656－715 页（1949 年 10 月）。

不幸的是，通常情况是两个用户（例如两名警官）并不事先同意共用一个秘密密钥。这使得通过古典密码系统甚至通过要求用户生成伪随机量的 PKC 系统来加密实时通信成为不可能。此外，流行的 PKC

系统是无法证明安全的，并受到计算复杂性上的严格要求及必须交换的信息量的困扰。随着攻击 PKC 系统的新方法的建立，PKC 系统将退却到甚至更长的交换矢量（实际上更大的素数）及甚至更复杂的计算。结果，对于许多通信情况，古典的与 PKC 密码系统不够理想。

除了提供安全性，花费许多精力来克服危害通信系统的不可避免的传输错误，能在数字通信系统中产生可怕后果的错误。对付这种错误的一种方法是采用能降低在接收机上的位错误的概率的纠错码。例如，将要传输的模拟信息转换成数字信息，然后按照块纠错码加以变换。如 D.Calcutt 等人在“卫星通信：原理与应用”136－161 页中所指出的，编码过程将包含要传输的信息的位与有时称作“冗余位”的其它位组装在一起，因为后者不包含信息但能协助检测与纠正错误。

许多现代数字通信系统采用这种纠错方案，其中包含诸如北美数字高级移动电话服务（D－AMPS）等蜂窝式无线电系统，它们的一些特征由电子工业协会与电信工业协会（EIA/TIA）及欧洲 GSM 系统所公布的 IS－54－B 与 IS－136 标准规定。

在这种时分多址联接（TDMA）系统中，将各无线电信道或无线电载波频率分成一系列时隙，每个时隙包含来自数据源的信息短脉冲串，诸如话音对话的数字编码部分。在各时隙中，可传输 324 位，其中的主要部分，260 位，是编码器/解码器（codec）的话音输出，包含话音输出的纠错编码位在内。其余的位用于诸如同步等目的的保护时间及开销信令。以类似方式发送控制信息。按照 IS－136 标准的数字控制信道上的时隙格式基本上与在 IS－54-B 标准下用于数字业务信道的格式相同，但新的功能与按照 1994 年 10 月 31 日提交的美国专利申请号 08/331，703 的各时隙中的字段一致。

其它通信方法采用称作码分多路复用（CDM）与码分多址联接（CDMA）的系统。在传统的 CDMA 系统中，通过组合信息序列与扩展序列而将要传递的数字信息序列扩展或映射到较长的数字序列中。结果用 N 个“片”值的序列表示信息序列的一或多位。在称作“直接扩展”的这一过程的一种形式中，各扩展符号主要是信息符号与扩展序列之积。在称作“间接扩展”的第二种扩展形式中，用不同的不一定相关的扩展序列来取代不同的可能信息符号。应理解信息符号可由信

道编码与/或扩展的前面的阶段产生。传统 CDMA 通信的各方面在下列文献中描述，K,Gilhousen 等人的“关于蜂窝式 CDMA 系统的容量”IEEE Trans. Veh. Technol. 卷 40，303－312 页（1991 年 5 月）；以及以下美国专利文件：颁给 Dent 的美国专利号 5，151，919；颁给 Dent 等人的专利号 5，353，352；及 1993 年 11 月 22 日提交的美国专利申请号 08/155，557。

按照本申请人的发明，利用通信信道的特征来建立与交换几乎完美无缺的密码密钥。这些特征为用户所见的信道阻抗，即从位置 A 向位置 B 观察的阻抗及从位置 B 向位置 A 观察的阻抗。对于非互易信道，这些阻抗通常不相等。可用等价于限定距离解码过程的计算来建立密钥，并且用来建立密钥的解码器可用来处理后面的数据传输。

因而，与古典的及 PKC 密码系统相比，本申请人的发明提供了依赖于物理过程来建立与共用密码密钥的替代机制。利用本申请人的系统，各方无须生成伪随机量，因为必要的随机性是由通信信道本身的不可预测的可变性提供。通过使用信道解码器，两个用户建立相同的秘密密钥的概率接近 1，而窃听者建立相同的密钥的概率基本上为零。这称作“概率保密性”。同时，可能的密钥的数目大到足以使用穷举搜索找到正确的密钥是不现实的。这称作“计算保密性”。这些概率测度与 Shannon 的完善保密测度不同。

在一方面，本申请人的发明为通过第一收发机与第二收发机之间的通信信道的安全通信提供建立密钥序列的方法。这一方法包括下述步骤，在第一收发机中，发送第一多个音调，各音调具有各自的预定频率及预定的初相；及在第二收发机中，接收第一收发机发送的第一多个音调，并基本上不加改变地将所接收的第一多个音调发送回第一收发机。以类似方式，第二收发机进行发送具有各自的预定频率及初相的第二多个音调的步骤，及在第一收发机中，接收第二多个音调并基本上不加改变地将所接收的第二多个音调发送回第二收发机。

这一方法还在第一收发机中包含下述步骤：确定所接收的音调对的相位之间的差；将各差量化成多个相位判定值中各自的一个；以及按照预定的块码将多个量化的差解码成一个密钥序列。以类似的方式，第二收发机进行下述步骤；确定所接收的音调对的相位之间的差；将各差量化成多个相位判定值中各自的一个；以及按照预定的块

码将多个量化的差解码成密钥序列。

按照本申请人的发明，第一与第二收发机所确定的密钥序列相同的概率基本上为 1。

该方法还可包括，在各第一与第二收发机中的下述步骤，确定其各自的多个音调的各个的幅值，其中这些幅值是在解码步骤中用作软信息的。并且该方法还可包括在第一与第二收发机中至少一个上按照该密钥序列加密要传输的信息的步骤；及在第一与第二收发机中的至少另一个中，按照该密钥序列解密加密的传输信息的步骤。

在本申请人的发明的另一方面中，为通过第一收发机与第二收发机之间的通信信道的安全通信建立密钥序列的方法包括下述步骤：在第一收发机中，发送包含多位的第一预定数字字；及在第二收发机中，接收第一预定数字字，并且无实质改变地将所接收的第一预定数字字发送回第一收发机。这一方法还包含下述步骤：在第二收发机中发送包含多位的第二预定数字字；及在第一收发机中接收第二预定数字字及基本上不加改变地将所接收的第二预定数字字发送回第二收发机。

本发明这一方面的方法还包括下述步骤：在第一收发机中硬判决解码从第二收发机接收的第一预定数字字中的多位中的各位；并按照预定的块码将硬判决解码的多位映射到密钥序列中；以及在第二收发机中，硬判决解码从第一收发机接收的第二预定数字字中的多位中的各位；并按照预定的块码将硬判决解码的多位映射到密钥序列中。

该方法可还包括，在各第一与第二收发机中，确定其各自接收的预定数字字的多位中各位的幅值的步骤，其中这些幅值在映射步骤中用作为软信息。

在本申请人的发明的另一方面中，为通过第一收发机与第二收发机之间的通信信道的安全通信建立密钥序列的方法包括下述步骤：在第一收发机中，发送包含多位的第一预定数字字；及在第二收发机中，接收第一收发机所发送的第一预定数字字及基本上不加改变地将所接收的第一预定数字字发送回第一收发机。该方法还包括下述步骤；在第二收发机中，发送包含多位的第二预定数字字；及在第一收发机中，接收第二收发机所发送的第二预定数字字，并基本上不加改变地将所接收的第二预定数字字发送回第二收发机。

在第一收发机中，确定从第二收发机接收的第一预定数字字的多位中各位的相位；确定各确定的相位与各自的预定相位之间的差；将各差量化成多个相位判定值中各自的一个；及按照预定的块码将多个量化的差解码成一个密钥序列。在第二收发机中，确定从第一收发机接收的第二预定数字字的多位中各位的相位；确定各确定的相位与各自的预定相位之间的差；将各差量化成多个相位判定值中各自的一个；及按照预定的块码将多个量化的差解码成密钥序列。

这一方法可还包括，在各第一与第二收发机中，确定其各自接收的预定数字字的多位中各位的幅值的步骤，其中这些幅值在解码步骤中用作软信息。

在各其它方面，本申请人的发明为第一收发机与第二收发机之间的安全无线通信建立密钥序列提供若干装置。

下面参照只作为示例给出并示出在附图中的实施例更详细地描述本申请人的发明，其中：

图 1 为展示通信系统的方框图；

图 2 为展示采用用于建立密钥序列的音调梳的通信系统；

图 3 示出相位空间判定区；

图 4 为采用用于建立密钥序列的导频符号的通信系统；

虽然以下的描述是在无线电话系统的上下文中的，熟悉本技术的人员会理解本申请人的发明也可应用在采用互易或非互易通信信道的其它通信系统中。

如本申请人 1995 年 1 月 20 日提交的美国专利申请号 08/376,144 及 1995 年 11 月 13 日提交的美国专利申请号 08/555,968 中所说的，本申请人的发明提供了用于建立两个序列，一个在发射机上另一个在接收机上，使得这两个序列落入多个“球”中同一个中具有高概率的方法与装置。通过引用将这些美国专利申请结合在此。这些“球”是由组装 M^n 个矢量 r 到 s 个球中的 t－球构成的，其中 t 为具有包含在 Galois 域 GF（$M=2^n$）中的元素的所有矢量，即其中 $r_i \in$ GF（$M=2^n$）的所有 $r=(r_1, r_2, \cdots, r_n)$，所构成的 n 维矢量空间的 Hamming 半径。（在本说明书中，矢量或序列是用黑体字表示的而标量与函数是用普通字型表示的。）将球中的矢量映射到由该球的中心构成的表示式中，并且 S 个表示式的集合为 $\{C_1, C_2, \cdots, C_s\}$。各表示式矢量 C_i

具有长度 n 并能映射到具有长度 mn 的二进制矢量 K 中，而对应的二进制矢量的集合为 $K\{K_1, K_2, \cdots, K_s\}$。

按照本申请人的发明，发射机与接收机以高概率建立包含在集合 K 中的公共序列 K_I，并利用序列 K_i 来扩展从发射机传递到接收机的信息序列。由于窃听者能确定该公共序列 K_I 的概率基本上为零，不需要加入额外的加密与解密算法来达到密码学安全性也能达到安全通信。按照本申请人的发明构造的球提高了发射机与接收机建立这一公共序列 K_I 的概率，认为通常发射机建立序列 r_T 而接收机建立不同的序列 r_R。如果序列 r_T，r_R 落入同一球中，便将它们映射到集合 K 中的同一序列 K 中。

序列建立

广义的通信链路包括两条通信信道：一条信道从第一用户的发射机到第二用户的接收机而一条信道从第二用户的发射机到第一用户的接收机。可以认为链路包含到达希望访问第一与第二用户交换的信息的窃听者的第三信道。这一简单情况描绘在图 1 中，其中示出第一用户 A、第二用户 B 与窃听者 E.

这些信道可以是也可以不是互易的，这便是说，在一个方向上通过信道观察的诸如阻抗等信道特征可具有也可不具有在另一方向上通过信道观察的该特征的相同值。如在本申请人的美国申请号 08/376，144 中所描述的，当在短时间标度上考虑时用于移动电话的典型无线电信道是互易的，因为在两个方向上通过信道观察诸如阻抗等信道特征是相同的，这便是说通过信道在两个方向上传播的信号经受相同的多径效应。反之，由于许多原因，诸如有线电话信道等其它通信信道即使在短时间标度上也不是互易的。例如，在分组交换通信系统中，在一个方向上通过信道传播的分组通常采用与在另一方向上传播的分组所采用的路径不同的路径。

对于这种非互易信道，从 A 向 B 观察信道阻抗（称作 Z_{AB}）、从 B 向 A 观察的信道阻抗（称作 Z_{BA}）及 AE 信道的阻抗 Z_{AE}、Z_{EA} 完全是不同的并可随时间变化。换言之，信道是非互易的，与诸如蜂窝式无线电话信道等其它种类的通信信道相反。对于互易信道，阻抗 Z_{AB} 与 Z_{BA} 相同，但这些阻抗仍然与 AE 信道的阻抗不同。各信道中的热噪声用增加的噪声项 $n_i(t)$，i=1, 2, 3, 表示，它们增加信道的非互易性。

下面描述建立密钥序列的两种方法。

音调梳

紧接在下面的描述涉及基本上同时的音调对的顺序传输，但如稍后所描述的，将会理解同时能传输两个以上音调。

参见图 2，假定诸如第一用户 A 的第一收发机在第 R 个信号间隔[RT，（R+1）T]期间传输包含具有频率 f_1 与 f_2 的两个正弦波及具有相等的初始相位偏移 ϕ 与能量 E 的信号 S（t）。所传输的信号 S（t）可用若干种方法中任何一种生成，例如通过放大与求和两个适当的振荡器 201、203 或一个频率合成器的输出信号，及通过调制载波信号将结果上变频到适当的传输频率。忽略调制，传输的信号 S（t）由下列表达式给出：

$$s(t) = \sqrt{2E/T}\cos(2\pi f_1 t + \phi) + \sqrt{2E/T}\cos(2\pi f_2 t + \phi)$$

在有线通信系统中，用诸如用户线路接口电路（SLIC）等适当器件将传输的信号 S(t)耦合在线路上，并且耦合的信号通过有线信道。到达诸如用户 B 等第二收发机上的信号的幅值与相位由诸如 SLIC 等器件及传输的信号在其到达第二收发机经过的路上的所通过的传输线路生成的等价阻抗确定。除了其它事物，还加上具有双边功率频谱密度 No/2 的白高斯噪声 n(t)。

按照本申请人的发明的一个方面，第二收发机基本上不加改变地简单地将接收的信号发送回第一收发机。从而，第二收发机简单地作为信号的转发器工作，用于建立它从第一收发机接收的密钥序列。由于转发这一信号，即将接收的信号传输回第一收发机，所需的部件是众所周知与传统的，图 2 中简单地用标记为转发器的框表示。

到达第一收发机的由第二收发机转发的信号的幅值与相位进一步由器件及信号回到第一收发机经过的路上所通过的传输线路的等效阻抗确定。第一收发机在必要时下变频与放大它从信道上得到的信号（图 2 中未示出下变频器与放大器），并将得出的信号 r(t)与其本机生成的 $\cos(2\pi f_1 t)$ 及 $\cos(2\pi f_2 t)$ 的版本相关。如图 2 所示，各相关可用适当的混合器 205、207 及在连续的时间间隔 $T = 1/2\pi f_i$ 期间积分混合器的输出信号的可复位积分器 209、211 进行，然而也可利用本技术中普通技术人员所知的许多其它器件。低通滤波器 213、215 传

统地滤波相关器所生成的输出信号来抑制和（上变频）信号以及可能由邻近的信号引起的分量。

假定正弦波 $\cos(2\pi f_1 t)$ 及 $\cos(2\pi f_2 t)$ 是正交的并至少相隔信道的相干带宽，第一用户在第 K 个信令间隔中接收的往返行程信号 $r_{AB,BA}(t)$ 由下列表达式给出：

$$r_{AB,BA}(t) = \alpha_{AB}\alpha_{BA}\sqrt{2E/T}\cos(2\pi f_1 t+\phi-\phi_{AB}-\phi_{BA}) + \alpha_{AB}\alpha_{BA}\sqrt{2E/T}\cos(2\pi f_2 t+\phi-\phi_{AB}-\phi_{BA})$$

其中上述等效阻抗项由下列表达式给出：

$$Z_{AB} = \alpha_{AB}e^{-j\phi_{AB}} \qquad Z_{BA} = \alpha_{BA}e^{-j\phi_{BA}}$$

会理解没有必要用正弦波信号来建立密钥序列。由于只需要确定相位差，便有可能利用具有预定形状的其它信号对，例如，脉冲串（矩形波）对。采用这种“音调”的系统的数学分析可能比上述的更复杂（可能需要傅里叶变换、子波变换或“音调”的其它频谱分解），但原理保持不变。因此，对于本申请，名词“音调”应理解为意味着比简单的正弦波信号更多含义。

在第一用户的收发机中，将经过滤波的相关器输出信号提供给差分相位检波器 217，后者为各时间间隔 T 生成上述表达式中的相位项之间的估计的差。将接连的相位差估计值提供给量化器 219，后者将若干预定值中相应的一个分配给各相位差估计值。按照本申请人的发明，只要求不同时间间隔的相位差估计值不互相相关。（在下文中，当并不产生二义性时，将去掉时间下标 K。）

收发机 A 中的差分相位检波器 217 生成的基带差分信号 U_A 由下列表达式给出：

$$U_A = 2\alpha_{AB}\alpha_{BA}Ee^{-j(\phi_{AB}-\phi_{BA})} + \alpha_{AB}N_1 + \alpha_{BA}N_2^* = X_A + jY_a$$

其中 N_1 与 N_2 为复数值的、具有零平均值及方差 $\sigma^2 = 2ENo$。的高斯分布的随机过程，而*表示共轭。如上所述，第一用户 A 将各相位差估计值量化成 M 个预定值之一，生成量化器输出信号 $Q(\phi^A)$。图 3 中示出对于 M = 4 的相位空间判定区。

差分相位检波器 217 可生成基带信号的瞬时幅值与相位的模拟或

数字测定值。适用的差分检波器为在颁给 DENT 的美国专利号 5，084，669 及颁给 Holmqvist 的美国专利号 5，220，275 中所描述的两个相位检波器的组合，通过引用将这两个专利明确地结合在此。

通过在各时间 K＝1，2，…n 上重复上述估计一量化过程，第一用户 A 建立一序列用下列表达式给出的量化的相位差估计值：

$$r_A = [\ Q(\Phi_1^A),\ Q(\Phi_2^A),\ \ldots,\ Q(\Phi_n^A)\ ].$$

将量化器 219 生成的这一值序列 r_A 存储在诸如随机存取存储器、移位寄存器或等效器件等缓冲器 221 中，后者具有由最小距离、纠错解码器 223 的参数确定的长度。收发机 A 中的纠错解码器 223 变换量化的差估计值序列并生成对应于用户 A 的接收机的密钥序列 K_A 的输出信号。

实际上，缓冲器 221 的大小是由要求的密钥序列的长度确定的。如果解码器 223 具有块长度 N 及维度 K，则对于本实施例，缓冲器延时为 N，其中的梳只包含在 N 个时间中的各个上同时传输的两个音调。如下所述，可以同时传输两个以上音调，而相应地减少缓冲器延时。例如，如果同时传输 T 个音调，一次可量化 T－1 个相位差而缓冲器延时为 N/（T－1）。

缓冲器 221 生成的矢量 r_A 具有 N 个元素，各元素为 M 进制的，而这一 N 元素矢量是对广泛的多种多样的最小距离解码器 223 中任何一种的输入．一种有用的解码器为限定距离解码器，它是在 R.Blahut 的错误控制码的理论与实践“第 7 章，Addison-Wesley，读物，MA(1983) 中所描述的低复杂性解码器。解码器 223 将缓冲器生成的 N 个符号映射到另外 N 个符号上，后者便是所关心的密码密钥序列，如下面要详细描述的。

会理解在收发机中进行的信号处理操作可用适当的数字信号处理（DSP）装置在数字域中执行。以这种配置，通过编程 DSP 装置来适当地处理所接收的信号的数字样本，几乎能检测到任何类型的调制，例如如在 Dent 等人的“多模式信号处理“的美国专利申请号 07/967,027 中所描述的，通过引用明确地将其包含在此。会理解 DSP 装置可实现为硬接线逻辑电路，或作为诸如应用专用的集成电路（ASIC）的集成数字信号处理器更好。当然可以理解，ASIC 可包含为

执行所要求的功能优化的硬接线逻辑电路，当速度或另一性能参数比可编程数字信号处理器的通用性更重要时，这是普遍选择的配置。

以类似于上述的方式与硬件，第二用户 B 从第二用户发送给第一用户及从第一用户返回时接收的由一对音调或音调梳构成的信号建立其自己的量化相位差估计值的序列 r_B。

可以理解两个用户必须在相对于信道的阻抗的时标可以忽略不计的时段中交换他们各自的音调对，即交换必须在阻抗改变之前完成，诸如在将信号分配给不同的通信路径之前。预期有线电话信道的时标比本发明人的先有申请中考虑的时标可观地长，在毫秒而不是在微秒的数量级上。此外，第一用户初始发送的音调的频率必须充分接近第二用户初始发送的音调的频率，以便使信道在这些频率上的实际双向阻抗基本上相同。

此外，可理解各收发机必须基本上不改变音调之间的相位差地返回另一收发机的信号。本上下文中的“基本改变“为与从实际信道阻抗 Z_{AB}、Z_{BA} 产生的相位效应相比明显的改变（诸如会导致不同的密钥序列）。类似地，在采用音调的幅值的系统中，各收发机必须基本上不改变幅值地返回另一收发机的信号。可以理解，在返回信号到始发收发机的过程中，接收收发机有可能在相位差上加上或减去偏移，或者有可能在幅值上作用增益，假定始发收发机知道这些改变的幅度，通常可认为它们是“基本改变”。

在这些条件下，并由于各用户发动的各信号在两个方向上通过通信信道，序列 r_A、r_B 落入同一球内的概率接近 1，并从而这些解码器的使用得到坚强的密钥分配方案。

从传输的信号中，窃听者 E 能得到基带差分信号及相位差估计值的序列 r_E，但不是由用户 A 与 B 之间的信道的双向实际阻抗所确定的那些。从而，序列 r_E 落入与序列 r_A、r_B 同一球中的概率基本上为零。

如上所述，所建立的三个序列或矢量 r_A、r_B 与 r_E 中各个是作为输入信号提供给各自的纠错解码器的。解码器生成的输出信号对应于密钥序列 K_A、K_B、K_E。注意在收发机 A、B 上不需要执行加密。解码器限制可能的密钥的数目来提高第一用户与第二用户建立相同的密钥的概率，如下面更详细地描述的。此外，音调 f_1、f_2 应具有充分分离的频率使它们的相位独立。

系统的安全性取决于用通过通信信道的通路解除音调的相位的相关性的程度。如果解除相关性基本上是完全的，则窃听者破译本系统必须进行的工作量接近对密钥序列 K_A、K_B 的穷举搜索。

可以理解，两个音调可具有相等的能量与相等的初始相位偏移，这是例如用锁相环容易得到的。通常，只要求这些参数是预定的，即对它们各自的收发机事先知道的。

并且，前面的分析只考虑在任何时间发送两个音调，但通常，梳可包含两个以上同时发送的音调而前面的分析可应用于这一音调梳的连续的对上。事实上，通过基本上同时发送适当数目的音调的梳及估计与量化各接连的音调对的相位差，便能一次生成所有序列 r_A、r_B。

两个或更多音调的同时传输是所希望的，因为它易于当时控制音调的初始相位，导致较不复杂的系统。尽管如此，只须“基本上同时”发送这些音调，这便是说，假定在这期间并未基本上改变信道的实际双向阻抗，各音调对可在不同的时间上发送。再者，在本上下文中的“基本改变”将是导致确定改变的密钥序列的改变。

再者，一对音调中的音调之间的频率分隔没有必要与另一对之间的频率分隔相同；换言之，“梳”可具有不均匀分隔的“齿”。同时，没有必要只考虑连续的音调的对；换言之，一对中的“齿”可被其它“齿”隔开. 如果，梳包含按递增频率排列的 10 个音调 $f_1, f_2, \cdots, f_{10}$，相位差随机变量的必要均匀分布可通过例如将音调 f_1 与 f_4；f_2 与 f_5；f_3 与 f_6；等等配对而得到。只须各对中的音调正交地分隔即可，即频率分隔必须充分，如上所述。

导频符号

不用如上所述传输音调梳，可以只根据诸如为同步第一收发机与第二收发机的操作而传输的位等多个导频符号来建立密钥序列 K_A、K_B。下面描述根据导频符号建立密钥的两种方法。

通过硬判决解码导频符号并将得出的解码的导频符号序列映射到一个球的中心而粗略地建立序列 K。确信第一用户解码的序列中的任何错误将与第二用户解码的序列中的错误相同。从而，这两个导频符号序列将被映射到同一球中并产生相同的密钥。即使第一与第二用户所解码的序列中的错误稍有不同，两个序列仍将以高概率映射到同一球中，产生相同的密钥。这一方法的可能缺点是为了使窃听者穷举

所有可能性在计算上困难，需要许多导频符号。如果导频符号是蜂窝式无线电话系统的同步位，当前认为至少需要 60 位。

可以理解，必要的导频符号没有必要一起发送，即没有必要利用连续的位，诸如 TDMA 信号的一个时隙中的所有同步位。例如，一个时隙中的任何一个或多个同步位可以与其它时隙中的任何一个或多个同步位一起使用。只要求所使用的位组（例如不同时隙中的位）分隔比上述信道的相干时间长的时间间隔。

根据导频符号建立密钥序列的更精密的方法采用信道状态信息而不用硬判决解码。在这一方法中，第一与第二用户内插已知的导频符号并以类似于上面对于根据音调梳建立密钥的方法所描述的方式量化内插器的输出。

例如，经过必要的下变换，放大与滤波从第一用户返回的信号之后，第二用户为信号中的预定数字字中的各位确定一个估计值，这些位可以是时隙的同步部分。当然，第一与第二用户可同意采用另一组已知位。第二用户确定各估计值与各自的预定位之间的差。然后将这些差估计值量化并提供给最小距离解码器。如上面结合通过发送音调梳建立密钥描述的。

图 4 为用于进行利用导频符号的这一“精密方法”的系统的方框图。在用户 A 的第一收发机中，用加密器 401 按照密钥序列加密要传输的数据。当然，在建立密钥序列之前，加密器将不加改变地简单地传递要传送的数据。多路复用器 403 将要传输的加密数据与已知的导频符号组合，这些符号可以是在传统电话中用于同步与开销信号的位。只需要以已知相位传输导频符号即可。将多路复用器 403 构成的交错的数据与导频符号的序列提供给用于将信息耦合到通信信道上的脉冲形成器或其它器件，通信信道通常以等效阻抗及加性白高斯噪声为特征。

在用户 B 的第二收发机上，接收第一收发机发送的信号并基本不加改变地将其简单地传输回第一收发机，如上所述。从而，第二收发机在图 4 中只作为标记为转发器的框来表示。第二收发机通过以上述方式修改该字的通信信道发送第一收发机的预定的数字字。

将从信道到达第一收发机的信号下变换或否则在必要时耦合与传递通过匹配的滤波器 407。用适当地控制的开关 409 或抽取器将匹

配的滤波器 407 生成的信号分成包含所接收的传输数据的信号及包含所接收的导频符号的信号。内插器 411 测定接收的导频符号的相位及形成各测定的相位之间的差，它们通常已旋转了信道的等效阻抗及各自的导频符号的已知传输相位。内插器 411 最好低通滤波这些差估计值。量化器 413 量化内插器 411 生成的差值，必要时将其存储在缓冲存储器 415 中来累积足够的差值，然后由解码器 417 解码而生成密钥序列，如上面对于图 2 所描述的。

还将内插器 411 生成的差值提供给诸如纠错解码器等解调器 419 用以恢复传输的数据。解调器 419 也接收传输的数据，它们可能已传递通过适用于同步差值与传输的数据的延时器件 421。假定所接收的数据在传输前是按照密钥序列加密的，便将解调器 419 生成的加密的传输数据与解码器 417 生成的密钥序列提供给解密器 423 供恢复传输的数据。

以类似于上面描述的方式及硬件，第二收发机根据其自己的发送给及由第一收发机返回的预定的字建立其自己的密钥序列，并且该密钥序列以高概率与第一收发机建立的密钥序列符合。从而，第二收发机能解密第一收发机加密的传输。

球组装与关联

假定 K 是给定的并且球是预定的，将任意序列射到球中的一般问题是 NP 困难（NP－hard）的，即该问题的计算复杂性是与可能的球数成正比的。对于安全传输与扩展的这一应用，球的数目是极大的。尽管如此，在候选序列 K（对应于球的表示 C）上施加简化结构可将计算复杂性降低到可接受的程度。

按照本申请人的发明，候选序列的集合限制在线性块纠错码的序列的集合上。然后用这一码的纠错能力，即该码能纠正的错误的数目，来确定球的半径，并能用适当的已知解码过程将接收的序列 r 映射到候选序列 K 上。

作为一个特定的示例，线性 Bose-Chaudhuri-Hocquenghem(BCH)码能用作候选序列 K 的集合；这些码能用 Peterson-Gorenstein-Zierler 过程或 Berlekamp-Massey 过程或任何解码循环码的过程以低复杂性解码，如上面提到的 R.Blahut 的书中所述。如果码参数为带有最小 Hamming 距离 d 及带有码符号字母表 GF（2^m）的（n,k），

则可从大小为 2^{mn} 的集合中建立长度为 mn 的候选序列。球的 Hamming 半径 t 或等价地码的纠错能力，是由 $t \leq [(d-1)/2]$ 给出的。（球没有必要是紧密组装的）。

序列 r_A、r_B 与 r_E 为对实现 Berlekamp-Massey 过程的纠错解码器的输入。解码器的输出为序列 K_A、K_B 与 K_E。再一次指出收发机不需要执行加密。解码器基本上限制了可能的序列的数目，从而提高了第一与第二用户之间的序列符号的似然性。可以指出如果信噪比（SNR）非常之高，则不需要解码器，这可能在实际的有线通信系统中不太困难获得。

在许多通信系统中，要传递的信息序列是为纠错而块编码的。在正交块编码中，将 N 个信息位转换成 2^N 个 N 位正交码字之一。解码这一正交码字包含将其与 2^N 个码字的集合所有成员相关。给出最高相关性的码字的二进制下标产生所要求的信息。例如，如果接收的 16 位码字与 16 个具有下标 0－15 的正交 16 位码字的各集合的相关性在第 10 个码字上产生最高相关性，基层信息信号便是 4 位二进制码字 1010（它在十进制记数中为整数十）。这一码称作[16, 4]正交块码。通过转换码字的所有的位，每一个码字可传送又一位信息。这种编码称作双正交块编码。

这种编码的显著特征在于利用快速 Walsh 变换（FWT）器件可高效地执行同时与集合中的所有正交块码字相关。在[128,7]块码的情况中，将 128 个输入信号样本变换成 128 点 Walsh 频谱，其中频谱中的各点表示输入信号样本与集合中码字之一的相关的值。颁给 Dent 的美国专利号 5, 357, 454 描述了适用的 FWT 处理器，通过引用将其结合在此。

采用解码器对于第一与第二用户是理想的，虽然如上所述并不严格要求，但使用解码器并不有助于窃听者。对于扩展传输的信息或解除接收的信息的扩展，可原封不动地使用解码器所生成的序列，或可使用整个或一部分序列的二进制表示。可以理解这一“扩展”并非指 CDMA 通信系统中进行的扩展而言。通常密钥序列不适用于作为 CDMA 扩展序列由于它们的不受控制的交叉相关性质，尽管本申请人的密钥序列能用来加密与解密在 CDMA 系统中传递的信息。当然，通过实现在本申请人的美国专利申请号 08/555,968 中描述的技术，这些密钥

序列能用作 CDMA 扩展序列.

本申请人的序列符合方法与装置提供了优越的计算保密性及概率保密性. 采用本申请人的发明，能够共用长的任意密钥序列，并且即使在通信“对话”期间也能改变密钥序列。在典型的通信系统中，在准备进行通信对话时至少每次在用户向通信系统注册或受到通信系统认证时会希望建立新的密钥序列，甚至更频繁，诸如在每次过去了预定的时间间隔时，便希望建立新的密钥序列。

替代使用线性块码，安全通信系统可采用各用户发送的 2M 个正交音调的梳。这一梳系统具有与块码系统相同的性能，但梳系统需要大得多的带宽，如正交信号所需要的，以及更复杂的频率合成器来生成音调。

在两种系统中，安全性的性能测度采用概率的，而与完善保密的 Shannon 测度不同。具体地，在块码系统中，两个用户建立相同的密钥序列的概率接近 1 而窃听者建立相同序列的概率基本上为零。这是概率保密性。同时，可能的密钥序列的数目大到足以使通过穷举搜索找到正确的序列是不现实的。这便是计算保密性。

虽然已描述与展示了本申请人的发明的特定实施例，应理解本发明不限于此。本申请设想了落入以下权利要求书所定义的本申请人的发明的精神与范围内的任何与所有修正。

说 明 书 附 图

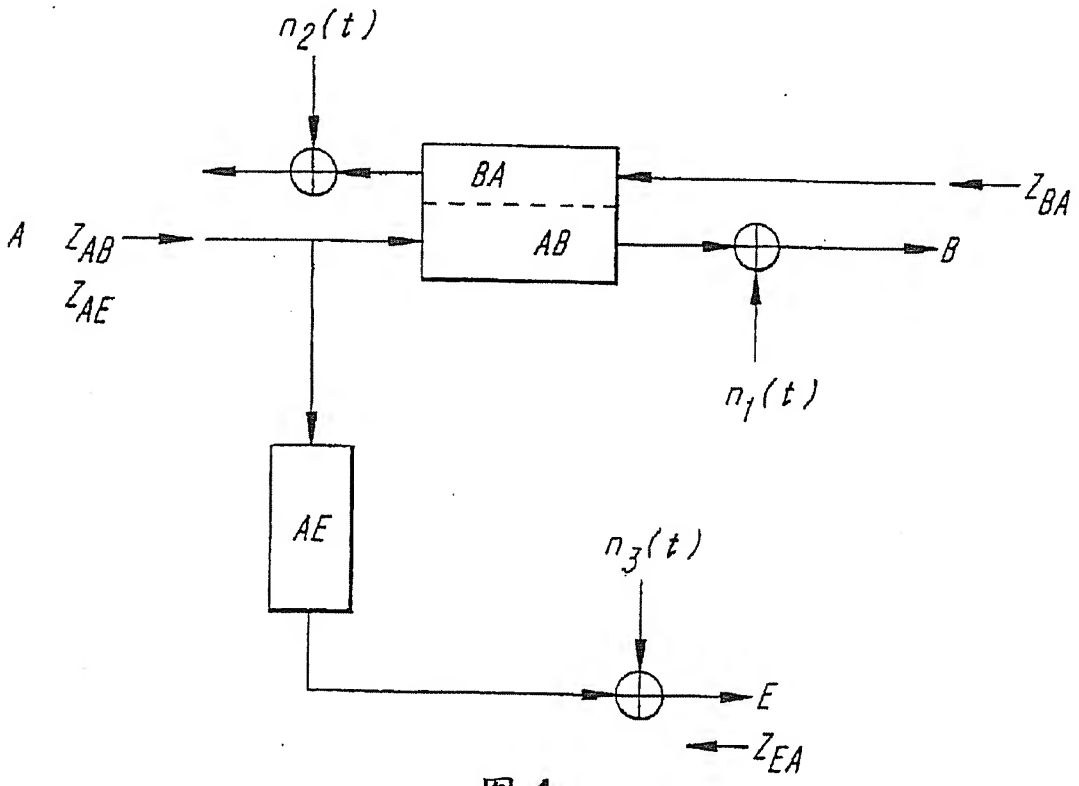


图 1

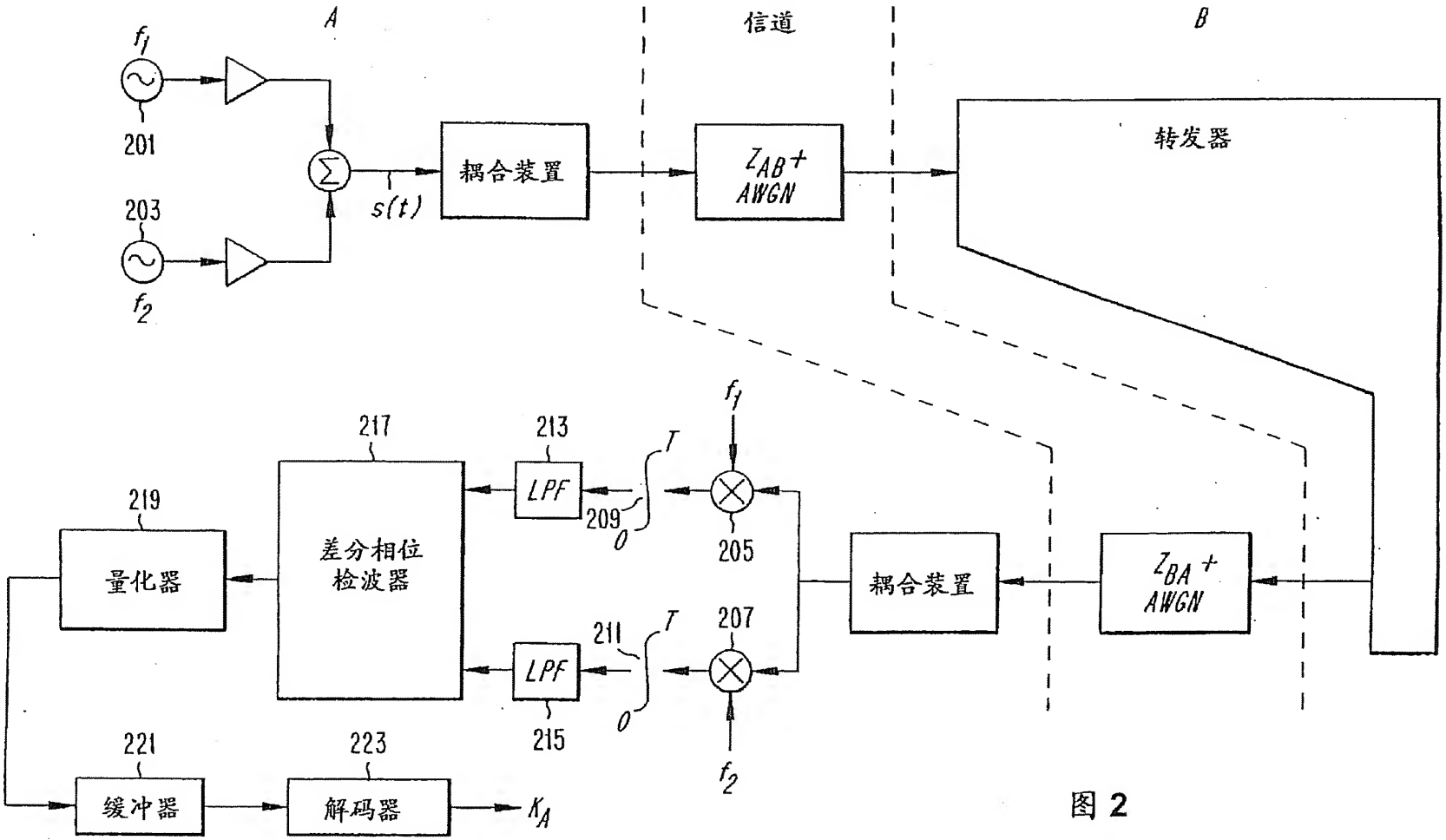

A
信道
B
f_1
201
203
f_2
$s(t)$
耦合装置
Z_{AB} + AWGN
转发器
217
213
LPF
T
209
0
f_1
205
219
量化器
差分相位
检波器
耦合装置
Z_{BA} + AWGN
211
T
207
LPF
0
215
f_2
221
223
缓冲器
解码器
K_A

图 2

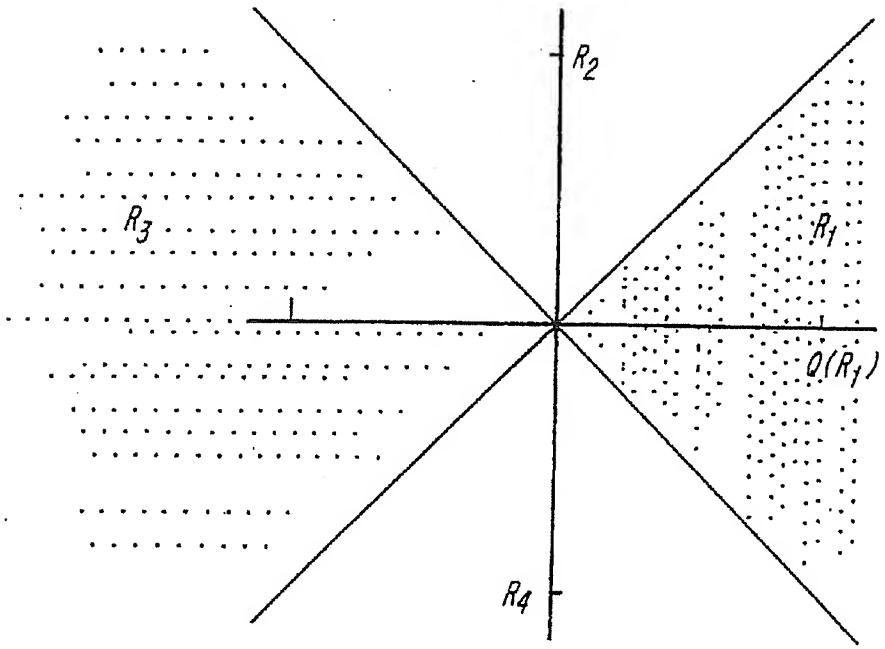


图 3

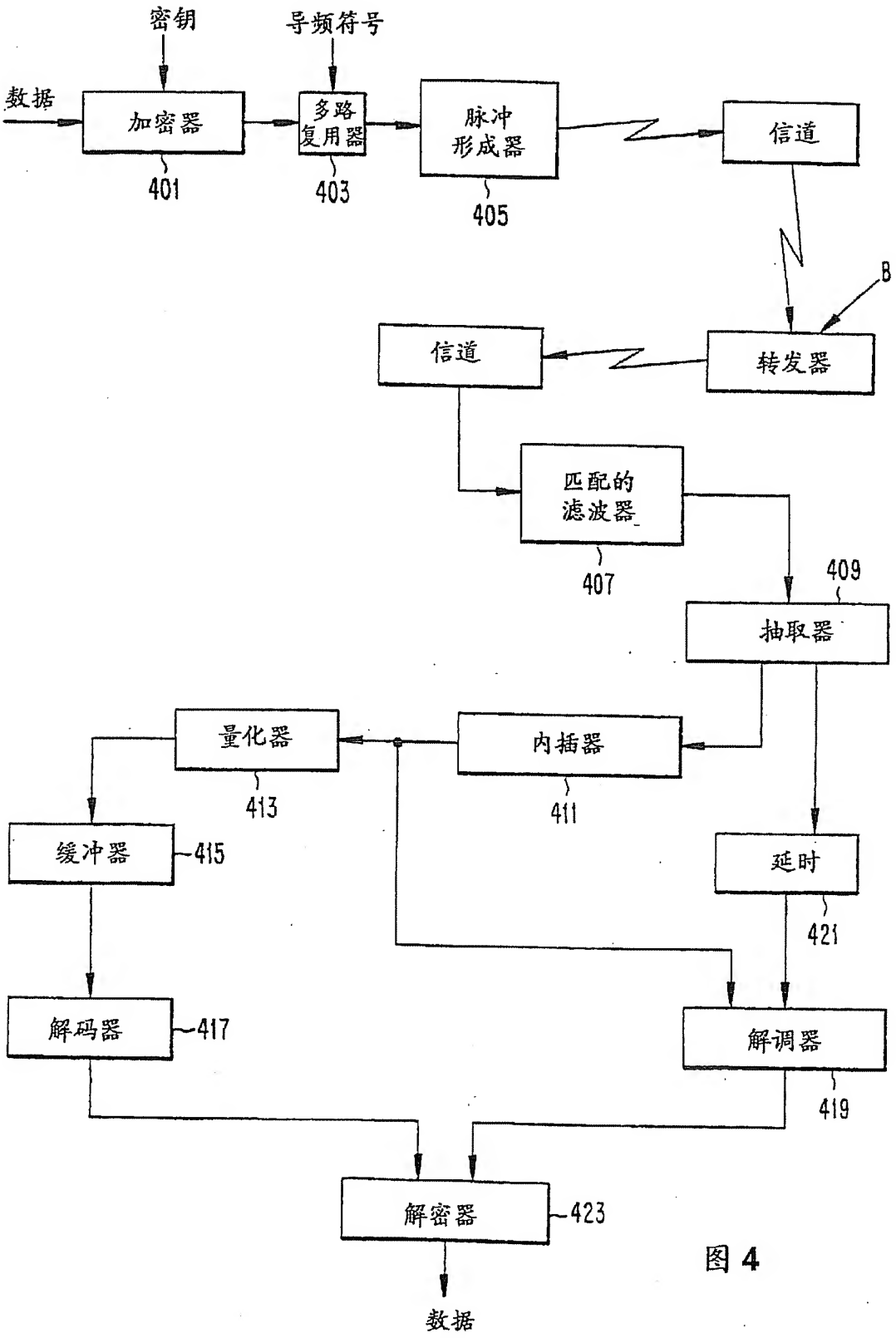

密钥
导频符号
数据
加密器
401
多路复用器
403
脉冲形成器
405
信道
B
转发器
信道
匹配的滤波器
407
409
抽取器
量化器
413
内插器
411
缓冲器
415
延时
421
解码器
417
解调器
419
解密器
423
数据

图 4